(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
7 février 2002 (07.02.2002)

PCT

(10) Numéro de publication internationale
WO 02/11363 A1

(51) Classification internationale des brevets[7] : H04L 9/32, G07F 7/10

(21) Numéro de la demande internationale :
PCT/FR01/02454

(22) Date de dépôt international : 26 juillet 2001 (26.07.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/10025 28 juillet 2000 (28.07.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gemenos, F-13420 Gemenos (FR).

(72) Inventeurs; et

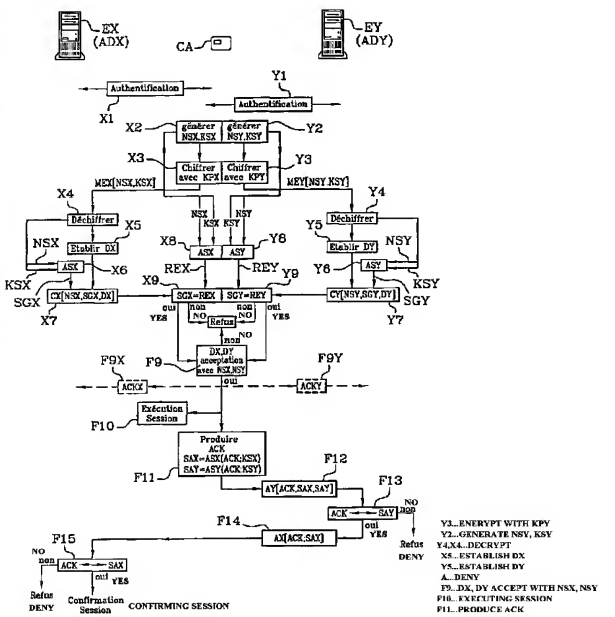
(75) Inventeurs/Déposants *(pour US seulement)* : **GIRARD, Pierre** [FR/FR]; 4, avenue de Brue, F-13600 la Ciotat (FR). **GIRAUD, Jean-Luc** [FR/FR]; Résidence Jardin des Potiers Bt A, F-13400 Aubagne (FR).

(74) Mandataire : **NONNENMACHER, Bernard**; Gemplus, Service brevets, Boîte postale 100, F-13881 Gemenos Cedex (FR).

[Suite sur la page suivante]

(54) Title: METHOD FOR MAKING SECURE A SESSION WITH DATA PROCESSING MEANS UNDER THE CONTROL OF SEVERAL ENTITIES

(54) Titre : SECURISATION DE SESSION AVEC UN MOYEN DE TRAITEMENT DE DONNEES SOUS LA COMMANDE DE PLUSIEURS ENTITES



(57) Abstract: The invention concerns a method for making secure the execution of a session with processing means, such as a smart card (CA), under the control of at least two entities, such as servers (EX, EY), which consists in: transmitting (X2, Y2) session numbers (NSX, NSY) and session keys (KSX, KSY) to the entities; applying (X6, X; Y6, Y8) the session number and key to an algorithm (ASX, ASY) in the processing means and the respective entity to produce a result (REX, REY) and signature (SGY, SGY); transmitting (X7, Y7) the numbers and the signatures to the processing means; and executing (F10) the session corresponding to the numbers from the processing means when the signatures are identical (X9, Y9) to the results. In another embodiment, one of the entities receives a delegation of a third entity to authorise execution of the session.

[Suite sur la page suivante]

WO 02/11363 A1

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : La sécurisation de l'exécution d'une session avec un moyen de traitement de données, tel que carte à puce (CA), sous la commande d'au moins deux entités, tels que serveurs (EX, EY), consiste à transmettre (X2, Y2) des numéros de session (NSX, NSY) et des clés de session (KSX, KSY) aux entités, appliquer (X6, X8; Y6, Y8) le numéro et la clé de session à un algorithme (ASX, ASY) dans le moyen de traitement et l'entité respective pour produire un résultat (REX, REY) et une signature (SGX, SGY), transmettre (X7, Y7) les numéros et les signatures au moyen de traitement, et exécuter (F10) la session correspondant aux numéros depuis le moyen de traitement lorsque les signatures sont identiques (X9, Y9) aux résultats. En variante, l'une des entités reçoit une délégation d'une troisième entité pour autoriser l'exécution de la session.

Sécurisation de session avec un moyen de traitement de données sous la commande de plusieurs entités

La présente invention concerne d'une manière générale la sécurisation de l'exécution d'une session avec un moyen de traitement de données sous la commande de première et deuxième entités électroniques.

Par exemple, le moyen de traitement de données est une carte à puce multi-applicative dans laquelle certaines ressources doivent être accessibles sous la condition qu'au moins deux entités donnent l'autorisation d'accéder à cette ressource. En effet, il est parfois intéressant de conditionner l'écriture dans un fichier d'une carte à puce ou de manière plus pratique le débit d'un compte dans une carte du type porte-monnaie électronique par l'autorisation de deux entités électroniques, tels que des serveurs de banque et de distributeur.

La présente invention vise précisément à sécuriser le déclenchement d'une session dans le moyen de traitement, telle que carte à puce, sous la commande d'au moins deux entités électroniques.

A cette fin, un procédé pour sécuriser l'exécution d'une session avec un moyen de traitement de données sous la commande d'au moins deux entités électroniques, est caractérisé en ce qu'il comprend les étapes suivantes de :

- transmettre des numéros de session et des clés de session depuis le moyen de traitement respectivement aux entités,
- appliquer le numéro de session respectif et la clé de session respective à un algorithme de

sécurisation respectif dans le moyen de traitement et l'entité respective pour produire un résultat respectif et une signature respective,

- transmettre le numéro de session respectif et la signature respective depuis l'entité respective vers le moyen de traitement, et

- exécuter la session depuis le moyen de traitement lorsque les signatures sont respectivement identiques aux résultats.

Afin que le moyen de traitement soit assuré que l'exécution de la session demandée corresponde bien au numéro de session transmis initialement, les résultats respectifs sont écrits en mémoire dans le moyen de traitement respectivement en correspondance aux numéros de session respectifs à transmettre aux entités, et sont lus en correspondance avec les numéros de session respectifs transmis par les entités vers le moyen de traitement avant d'être comparés aux signatures respectives.

En pratique, chacune des entités transmet vers le moyen de traitement des données respectives avec le numéro de session respectif et la signature respective. Les données contiennent une acceptation ou un refus d'exécuter la session. Ainsi, la session est exécutée si, en outre, le moyen de traitement détecte dans chacune des données une acceptation de la session par l'entité respective.

Selon une deuxième réalisation, la session est exécutée à condition que l'une desdites au moins deux entités ait reçu respectivement une délégation d'exécution de session par une troisième entité. Dans cette deuxième réalisation, le procédé comprend les étapes suivantes de :

- transmettre des informations de délégation respectives en faveur de l'une desdites au moins deux entités depuis une troisième entité électronique au moyen de traitement,

- transmettre un numéro de session, lequel est identique aux numéros de session respectifs, et une troisième clé de session depuis le moyen de traitement à la troisième entité prédéterminées,

- retransmettre le numéro de session et la troisième clé de session par la troisième entité vers ladite une entité, et

- appliquer non seulement le numéro de session, et la clé de session respective pour ladite une entité mais également la troisième clé de session à l'algorithme de sécurisation respectif dans ladite une entité et le moyen de traitement pour produire la signature respective et le résultat respectif.

Afin que ladite une entité soit certaine que la session dont l'exécution est demandée soit validée par la troisième entité, le numéro de session retransmis par la troisième entité et le numéro de session transmis directement par le moyen de traitement à ladite une entité sont comparés dans ladite une entité, et au moins l'étape d'appliquer dans ladite une entité n'est exécutée que lorsque les numéros de session comparés sont identiques.

La délégation peut être transmise à plus d'une entité. Ainsi, au moins une autre entité desdites au moins deux entités est déléguée de la troisième entité afin que la session ne soit exécutée que lorsque les signatures et les résultats produits en fonction du numéro de session, des clés de session respectives et de la troisième clé sont respectivement identiques.

D'autres caractéristiques et avantages de la présente invention apparaîtront plus clairement à la lecture de la description suivante de plusieurs réalisations préférées de l'invention en référence aux dessins annexés correspondants dans lesquels :

- la figure 1 est un bloc-diagramme schématique de plusieurs entités électroniques et d'un moyen de traitement de données de type carte à puce dans un réseau de télécommunication pour la mise en oeuvre du procédé de sécurisation selon l'invention ;
- la figure 2 est un algorithme d'étapes du procédé de sécurisation avec le moyen de traitement de données et deux entités électroniques selon une première réalisation de l'invention ; et
- la figure 3 est un algorithme d'étapes du procédé de sécurisation avec le moyen de traitement de données et une troisième entité électronique déléguant aux deux entités précédentes, selon une deuxième réalisation de l'invention.

A la figure 1 est représenté un réseau de télécommunication RT désignant dans leur ensemble tous les types de réseau de télécommunication tel qu'un réseau de radiotéléphonie, le réseau téléphonique commuté, un réseau numérique à intégration de service RNIS, un réseau à haut débit tel qu'un réseau ATM ou le réseau Internet, un réseau de transmission par paquets, etc. Le réseau RT constitue un moyen de communication entre un moyen de traitement de données CA et diverses entités électroniques dont trois sont représentées EX, EY et EZ.

A titre d'exemple auquel on se référera par la suite, le moyen de traitement de données est un contrôleur, tel que le microcontrôleur d'une carte à

puce CA, dans lequel doit être initié une session qui peut être une tâche à exécuter dans le moyen de traitement de données lui-même ou bien un échange d'unités de données, telles que messages, avec au moins l'une des entités EX, EY et EZ. Ainsi, le moyen de traitement de données peut être non seulement une carte à puce, dite également carte à microcontrôleur, mais également tout autre objet électronique portable, tel qu'assistant ou organiseur électronique, porte-monnaie électronique, jeton, calculette.

Une entité électronique, par exemple l'entité EX ou EY, est un serveur distant de la carte CA, par exemple appartenant à l'éditeur de la carte CA ou en relation avec l'une des applications implémentées dans la carte CA.

En variante, les entités EX et EY sont elles-mêmes des cartes à puce logées dans des lecteurs additionnels inclus dans des serveurs distants de la carte CA afin que deux administrateurs, possesseurs des cartes à puce, autorisent une session par la carte à puce d'un utilisateur.

L'entité EZ peut être un terminal d'accueil TA de la carte à puce CA, tel qu'un terminal bancaire, un terminal point de vente, ou un terminal radiotéléphonique mobile doté d'un lecteur de carte additionnel, ou bien encore un troisième serveur comme cela est prévu dans la deuxième réalisation décrite plus loin.

Selon une première réalisation du procédé de l'invention, l'exécution d'une session avec la carte à puce CA est sécurisée sous la commande de deux entités EX et EY.

Par exemple, la carte à puce CA est une carte avec un compte de points de fidélité éditée par une société distributrice de carburant. Après introduction dans un terminal TA d'une station service, en tant qu'entité EZ, la carte CA n'est autorisée à être débitée que par les deux entités EX et EY afin que le titulaire de la carte reçoive l'article de son choix correspondant à un débit de points. La première entité EX est un serveur de fournisseur d'article qui autorise simplement la carte CA à être débitée après reconnaissance de celle-ci. La deuxième entité EY est un serveur appartenant à la société distributrice du carburant qui vérifie non seulement l'identité de la carte CA mais également le compte de points contenu dans celle-ci avant d'autoriser le débit du compte dans la carte CA. Ainsi, la session consistant ici à débiter le compte de points de fidélité dans la carte CA n'est autorisée qu'après l'identification de la carte par les deux entités EX et EY et l'acceptation du débit par l'entité EY, ou de manière plus globale après l'acceptation de l'exécution de la session "débit de points" par les deux entités EX et EY.

Selon un autre exemple, le possesseur de la carte CA doit obtenir l'autorisation de deux autres possesseurs de cartes à puce, en tant qu'entités EX et EY, par exemple pour accéder à des fichiers prédéterminés dans un réseau Intranet. Les cartes "administratrices" EX et EY sont alors introduites dans les lecteurs de terminaux du réseau afin de transmettre à la carte CA une acceptation ou un refus de la session en fonction de droits d'accès aux fichiers prédéterminés.

Il est supposé préalablement que la carte à puce CA est de préférence pro-active et peut ainsi déclencher elle-même des actions vers le monde extérieur constitué notamment par le réseau de télécommunication RT à travers le terminal d'accueil TA qui est alors transparent à ces actions, bien qu'en variante certaines actions puissent être déclenchées par le terminal d'accueil TA lui-même. La carte CA par nature a un lien privilégié avec les entités EX et EY et contient en mémoire non volatile EEPROM des adresses de destinataire ADX et ADY des entités EX et EY, telles que leurs numéros téléphoniques d'appel ou leurs adresses IP (Internet Protocol). La mémoire non volatile de la carte CA contient également des clés publiques de chiffrement KPX et KPY respectivement associées aux entités EX et EY.

Le procédé de sécurisation selon la première réalisation montrée à la figure 2 comprend d'abord deux jeux d'étapes X1 à X9 et Y1 à Y9 qui sont respectivement associées à des échanges entre la carte CA et la première entité EX d'une part, et la carte CA et la deuxième entité EY d'autre part, puis des étapes finales F9 à F15. Les étapes X1 à X9 étant respectivement identiques aux étapes Y1 à Y9, le procédé est d'abord décrit en détail seulement pour des échanges entre la carte CA et la première entité EX.

Dès que la carte CA décide d'exécuter une session, par exemple à la suite d'une demande du terminal d'accueil TA, la carte CA initie une authentification de la carte CA par la première entité EX, à l'étape X1. L'authentification est classique et consiste essentiellement à transmettre

un nombre aléatoire par la première entité EX à la carte CA et à comparer dans l'entité EX les résultats de l'application de ce nombre aléatoire et d'une clé d'authentification pré-mémorisée dans la carte CA et l'entité EY, effectuée à la fois dans la carte CA et l'entité EX. Inversement, la carte CA authentifie l'entité EX. Plus complètement en variante, l'authentification est mutuelle, c'est-à-dire l'authentification comprend une authentification de la carte CA par l'entité EX, et une authentification de l'entité EX par la carte CA.

En variante, le procédé de sécurisation ne contient aucune authentification.

Si après authentification optionnelle la carte CA ne reçoit aucun message d'invalidation, la carte CA génère une clé de session KSX qui peut être aléatoire et associe à celle-ci un numéro de session NSX à l'étape X2. Puis après avoir mémorisé la clé KSX et le numéro NSX en correspondance, la carte CA prépare un message à transmettre à l'entité EX, contenant le numéro de session respectif NSX et la clé de session respective KSX qui ont été chiffrés au moyen de la clé de chiffrement publique respective KPX. Le message chiffré MEX ainsi constitué est transmis par la carte CA à l'entité EX à l'étape X3.

Après déchiffrement du message énoncé en fonction d'une clé privée de déchiffrement correspondant à la clé publique de carte KPX à l'étape X4, l'entité EX établit des premières données DX notamment pour marquer son acceptation de la session à exécuter, ou le cas échéant son refus, à l'étape X5. Puis l'entité EX détermine une signature SGX résultant de l'application du numéro de session NSX et de la clé de session KSX reçus à un premier algorithme de sécurisation ASX, à l'étape X6.

L'entité EX construit un message de commande CX qui contient le numéro de session NSX, la signature SGX = ASX (NSX, KSX) et les données DX et qui est transmis à la carte CA à l'étape X7. Le contenu du message de commande CX est de préférence chiffré de manière analogue à celui du message MEX.

Dans la carte CA, après la transmission du message chiffré MEX à l'étape X3, est déterminé également un résultat REX de l'application du numéro de session NSX et de la clé de session KSX au premier algorithme de sécurisation ASX, à l'étape X8. Le résultat REX est écrit en mémoire non volatile dans la carte CA jusqu'à ce qu'il soit lu à l'étape X9, en réponse au message de commande CX. A cette étape X9, la signature SGX reçue par la carte et correspondant au numéro de session NSX est comparée au résultat REX mémorisé dans la carte. Si la signature SGX est différente du résultat REX, la session demandée par le terminal TA avec la carte CA est refusée par celle-ci.

Sinon, lorsque la signature SGX est identique au résultat REX, le procédé passe aux étapes finales dans la mesure où les étapes Y1 à Y9 aboutissent également à une étape Y9 selon laquelle une deuxième signature SGY transmise par l'entité EY est identique à un deuxième résultat REY déterminé par la carte CA. Comme cela apparaît dans la figure 2, les étapes Y1 à Y9 sont déduites des étapes précédemment décrites X1 à X9 en remplaçant la lettre X par la lettre Y. Ainsi, le deuxième résultat REY résulte de l'application dans la carte CA d'un deuxième numéro de session NSY et d'une clé de session KSY qui peut être aléatoire, générés à l'étape Y2 par la carte CA, à un deuxième algorithme de sécurisation ASY. La deuxième signature SGY résulte de l'application dans

la deuxième entité EY à l'étape Y4, du numéro de session NSY et de la clé de session KSY transmis sous forme chiffrée dans un message MEY par la carte CA à l'étape Y3, au deuxième algorithme de sécurisation ASY. La deuxième entité EY transmet à l'étape Y7 également dans un message de commande CY de préférence chiffré, le numéro NSY et la signature SGY ainsi que des deuxièmes données DY traduisant l'acceptation de l'exécution de la session par l'entité EY, ou un refus de celle-ci.

Après une identité de la première signature SGX et du premier résultat REX à l'étape X9 et une identité de la deuxième signature SGY et du deuxième résultat REY à l'étape Y9, la carte CA compare les données DX et DY à l'étape F9. Si l'une ou l'autre des données DX et DY représente un refus, ou bien si l'un NSX ou l'autre NSY des numéros de session retransmis par les entités EX et EY est différent du numéro attribué à l'étape X2 ou Y2, la session demandée n'est pas exécutée. Sinon, les données DX et DY représentent une acceptation de la session correspondant aux numéros reçus NSX et NSY par les entités EX et EY et le procédé est poursuivi par l'exécution de la session à l'étape F10.

Selon d'autres variantes de la première réalisation, le premier numéro de session NSX attribué à l'échange de données entre la première entité EX et la carte CA, et le deuxième numéro de session NSY attribué à l'échange de données entre la carte CA et la deuxième entité EY sont identiques, et les premier et deuxième algorithmes de sécurisation ASX et ASY sont identiques.

Selon une première variante d'étapes finales montrée en traits interrompus courts à la figure 2,

la carte à puce CA transmet des accusés de réception respectifs ACKX et ACKY aux première et deuxième entités EX et EY lorsqu'à la fois la première signature SGX est identique au premier résultat REX et la deuxième signature SGY est identique au deuxième résultat REY, aux étapes X9 et Y9. De préférence, la transmission des premier et deuxième accusés de réception ACKX et ACKY intervient plutôt après l'étape finale F9, lorsque la carte CA a détecté dans les premières et deuxièmes données DX et DY une acceptation de la session par les entités EX et EY. Grâce à ces deux accusés de réception, les entités EX et EY savent chacune que l'autre entité a accepté la session. La session peut être exécutée à l'étape suivante F10 comme illustré à la figure 2, ou en variante précédemment aux transmissions des accusés de réception ACKX et ACKY.

Selon une deuxième variante d'étapes finales, après le constat des identités de signature et de résultat aux étapes X9 et Y9, de préférence après la détection d'une acceptation de la session par les entités EX et EY, la carte CA produit à une étape F11 un mot ACK représentatif de la session à exécuter à une étape F10. A cet égard, la session peut être exécutée à l'étape F10 avant la transmission du mot ACK à l'étape F11 comme illustré à la figure 2, ou en variante après l'étape F11.

Plus précisément, selon cette deuxième variante, la carte CA produit une première signature de mot SAX résultant de l'application du mot représentatif ACK et de la première clé de session KSX au premier algorithme de sécurisation ASX, et une deuxième signature de mot SAY résultant de l'application du mot représentatif ACK et de la deuxième clé de session KSY au deuxième algorithme de sécurisation

ASY. La carte CA encapsule le mot ACK et les signatures de mot SAX et SAY dans un message AY pour le transmettre à l'une des entités, par exemple la deuxième entité EY, à une étape F12.

La deuxième entité EY vérifie la correspondance entre le mot reçu ACK représentatif de la session et la deuxième signature de mot respective SAY en fonction de la clé de session respective KSY qui avait été reçue et mémorisée dans l'entité EY à l'étape Y4, en appliquant le mot reçu ACK et la clé KSY au deuxième algorithme ASY de manière à produire un résultat qui est comparé à la deuxième signature reçue SAY, à une étape F13. Si cette comparaison est positive, c'est-à-dire si le mot reçu ACK correspond à la signature SAY, la deuxième entité EY transmet un message AX contenant le mot ACK représentatif de la session et l'autre signature, c'est-à-dire la première signature de mot SAX = ASX (ACK ; KSY), à l'autre entité EX à une étape F14. A la réception du message AX, la première entité EX vérifie la correspondance entre le mot représentatif ACK et la première signature de mot reçue SAX en fonction de la clé de session respective KSX qui avait été reçue et mémorisée dans l'entité EX à l'étape X4. Cette vérification consiste à appliquer le mot reçu ACK et la première clé de session KSX au premier algorithme de sécurisation ASX et à comparer le résultat produit par cet algorithme avec la signature reçue SAX à une étape F15.

Si à l'étape F13, l'entité EY constate un défaut de correspondance entre le mot représentatif de session ACK et la deuxième signature de mot SAY, l'entité EY ignore le résultat de la session exécutée et ne transmet pas le message AX à l'entité EX ou bien transmet un message d'accusé négatif à l'entité

EX ; en variante, l'entité EY procède également à une annulation de la session lorsqu'elle est encore à exécuter dans la carte CA via le terminal TA. De même, lorsque la première entité EX constate un défaut de correspondance entre le mot représentatif de session ACK et la première signature de mot SAX, l'entité EX ignore le résultat de la session exécutée et le signale de préférence à l'entité EX ; en variante, l'entité EX procède également à une annulation de la session dans la carte CA lorsqu'elle est à exécuter.

En variante, les messages d'accusé réception ACKX et ACKY, et/ou les messages AX et AY sont chiffrés.

Bien que la première réalisation ait été décrite avec deux entités EX et EY, l'invention englobe également des réalisations avec plus de deux entités qui chacune doit donner son acceptation à la carte CA selon les étapes X1 à X9, Y1 à Y9 pour autoriser l'exécution de la session. En particulier, pour la deuxième variante montrée au bas de la figure 2, l'étape F11 produit autant de signatures de mot SAX, SAY qu'il y a d'entités EX, EY, et chacune de ces entités effectue une étape F13, F15 au cours de laquelle elle vérifie la correspondance entre le mot ACK représentatif de la session et la signature de mot respective SAX, SAY en fonction de la clé de session respective KSX, KSY, et ainsi de suite jusqu'à la dernière entité.

Selon une deuxième réalisation du procédé de sécurisation selon l'invention, une troisième entité électronique EZ intervient. Lorsque la carte CA décide d'exécuter une session prédéterminée, elle

interroge systématiquement la troisième entité EZ qui ne possède pas assez d'information pour décider si elle accepte ou non la session demandée ; l'entité EZ délègue alors cette décision pour une durée prédéterminée aux première et deuxième entités EX et EY en leur transmettant des premières et deuxièmes informations de délégation IDX et IDY respectivement.

Selon une variante complémentaire, si les commandes exécutées dans la session de l'étape F10 nécessitent l'intervention de l'entité EZ et si l'entité EZ ne pourra/voudra pas intervenir dans cet échange interactif, la délégation permet à l'entité EZ de signifier à la carte CA que l'entité EX, EY qui a reçu la délégation a le droit d'agir au nom et pour le compte de l'entité EZ.

Par exemple comme montré à la figure 1, la troisième entité EZ, le délégant, est un serveur d'une banque qui pendant une période de congé annuelle autorise un crédit au possesseur de la carte CA, et par suite fait confiance à un premier serveur EX d'un site commercial connecté au réseau Internet et présentant des produits à acheter et également à un deuxième serveur EY d'un livreur de produits. Lorsque l'usager, le délégataire, décide, par l'intermédiaire de son propre terminal informatique TA relié au réseau RT et doté d'un lecteur de carte additionnel dans lequel est introduite la carte CA, d'acheter un produit auprès du serveur EX, cette transaction est déclenchée par le serveur de banque EZ qui a vérifié que le compte correspondant à la carte à puce CA a un crédit autorisé et qui fait relayer la transaction par les serveurs EX et EY, les délégués, dans la mesure où ces derniers ont reçu une validation sous la forme d'une clé KSZ fournie par la

carte CA et retransmise par le serveur EZ, comme on le verra ci-après.

Il est supposé dans cette deuxième réalisation que les entités EX et EY ont déjà eu connaissance de la délégation transmise par la troisième entité EZ.

Comme cela apparaît en comparant les figures 2 et 3, la deuxième réalisation du procédé selon l'invention comprend d'abord des étapes Z1 à Z7 relatives à des échanges de données entre la troisième entité EZ et la carte à puce CA. De manière analogue à la première réalisation, la carte CA contient en mémoire non volatile les adresses de destinataire ADX, DAY et ADZ des entités EX, EY et EZ ainsi que des clés publiques de chiffrement KPX, KPY et KPZ associées à ces entités.

A la première étape Z1, suite à une demande d'exécution de session par la carte CA transmise à l'entité EZ, l'entité EZ authentifie la carte CA, ou en variante l'entité EZ et la carte CA s'authentifient mutuellement.

En variante, la deuxième réalisation du procédé de sécurisation ne contient aucune authentification.

Après authentification optionnelle, l'entité EZ fournit les premières et deuxièmes informations de délégation IDX et IDY à la carte CA. Chacune des premières et deuxièmes informations de délégation contient par exemple l'adresse ADX, ADY, ou autre identificateur de délégué, de l'entité EX, EY, et le nombre de pouvoirs requis pour exécuter la session, c'est-à-dire le nombre d'entités telles que les entités EX et EY dont l'acceptation est requise pour exécuter la session. Ainsi, à l'étape Z2, la troisième entité EZ transmet les premières et deuxièmes informations de délégation IDX et IDY ainsi que l'adresse de source ADZ de l'entité EZ à la carte

CA sous la forme d'un message qui est signé avec la clé privée de la troisième entité EZ correspondant à la clé publique KPZ, puis chiffré avec la clé publique KPCA de la carte CA. Après déchiffrement, vérification de signature et mémorisation des informations IDX et IDY à l'étape Z3, la carte CA génère un numéro de session NS ainsi que trois clés de session KSX, KSY et KSZ qui peuvent être aléatoires, et les associe respectivement aux entités EX, EY et EZ en correspondance avec le numéro de session NS, à l'étape Z4. Ces quatre paramètres NS, KSX, KSY et KSZ sont mémorisés dans la carte afin de servir dans les étapes ultérieures.

A l'étape suivante Z5, la carte CA chiffre le numéro de session NS et la troisième clé de session KSZ avec la clé de chiffrement KPZ pour les transmettre dans un message chiffré MEZ à la troisième entité EZ. Après déchiffrement du message MEZ et mémorisation du numéro NS et de la clé de session KSZ à l'étape Z6, l'entité EZ établit deux messages MZX et MZY transmis respectivement vers les entités EX et EY. Le premier message MZX comprend le numéro de session NS et la troisième clé de session KSZ et l'adresse de destination ADX qui sont chiffrés au moyen de la clé publique KPX de la première entité EX. Le deuxième message MZY comprend également le numéro NS, la clé KSZ et l'adresse ADY qui sont chiffrés au moyen de la clé publique KPY de la deuxième entité EY. Les messages MZX et MZY sont respectivement reçus par les entités EX et EY pour y être déchiffrés au moyen de leurs clés privées de chiffrement et y être mémorisés à des étapes suivantes Z8X et Z8Y.

Parallèlement aux étapes Z4 à Z7, la carte CA effectue des étapes X1 à X4 et Y1 à Y4, sensiblement

identiques à celles déjà décrites en référence à la figure 2, en réponse aux informations de délégation IDX et IDY reçues à l'étape Z3, de manière à authentifier la carte CA par les entités EX et EY déléguées par l'entité EZ et à transmettre des messages chiffrés MEX[NS, KSX] et MEY[NS, KSY] par la carte CA aux entités EX et EY et à déchiffrer ces messages aux étapes X4 et Y4.

Puis à une étape Z9X, Z9Y dans l'entité EX, EY, le numéro de session NS mémorisé à l'étape Z8X, Z8Y et transmis par la troisième entité EZ est comparé au numéro de session NS et transmis par la carte CA et déchiffré à l'étape X4, Y4, par analogie à la comparaison du numéro de session reçu et mémorisé NSX, NSY à l'étape F9. Si les numéros de session sont différents, l'entité EX refuse la session demandée. Sinon, les deux numéros de session sont identiques et des données DX, DY représentatives d'une acceptation de la session par l'entité déléguée EX, EY à l'étape X5, Y5 sont établies. Le procédé est poursuivi par des étapes X6Z et X7Z, Y6Z et Y7Z remplaçant respectivement les étapes X6 et X7, Y6 et Y7, et se distinguant de celles-ci par le fait que la signature SGXZ, SGYZ est déterminée en appliquant le numéro de session NS validé à l'étape précédente Z9X, Z9Y, la clé de session KSX, KSY reçue et déchiffrée à l'étape X4 et la troisième clé de session KSZ reçue, déchiffrée et mémorisée à l'étape Z8X, Z8Y, à l'algorithme de sécurisation ASX, ASY. Le numéro de session NS, la signature SGXZ, SGYZ et les données DX, DY sont de préférence chiffrés et encapsulés dans un message CXZ, CYZ qui est transmis à la carte CA.

Parallèlement aux étapes X4 à X7Z, Y4 à Y7Z, un résultat REXZ, REYZ est déterminé dans la carte à une étape X8Z, Y8Z remplaçant l'étape X8, Y8, en

appliquant à l'algorithme de sécurisation ASX, ASY le numéro de session NS, la clé KSX, KSY et la troisième clé KSZ.

L'étape suivante X9Z, Y9Z dans la carte CA compare la signature SGXZ, SGYZ au résultat REXZ, REYZ de manière à passer à l'étape finale F9 lorsque les identités SGXZ = REXZ et SGYZ = REYZ sont vérifiées.

Grâce à la transmission de la troisième clé KSZ par la carte CA à travers la troisième entité EZ et la transmission des clés KSX et KSY par la carte CA directement aux entités EX et EY, la transmission des signatures SGXZ et SGYZ dépendant de ces deux couples de clés avec des données d'acceptation DX et DY à la carte CA assurent que les entités EX et EY ont récupéré la délégation de l'entité EZ et sont autorisées à donner l'ordre d'exécution de la session de numéro NS par délégation.

Selon une troisième réalisation combinant les première et deuxième réalisations, seulement l'une des entités EX et EY, par exemple la première entité EX, est déléguée de la troisième entité EZ. Une session n'est exécutée que lorsque la carte CA a reçu l'acceptation de l'entité EX par délégation de l'entité EZ et l'acceptation de l'entité EY indépendante de l'entité EZ.

Pour la troisième réalisation, la partie gauche de l'algorithme de la figure 3 par rapport à la carte CA, c'est-à-dire les étapes Z1 à Z7 en supprimant IDY(ADY), KSY et KPY et les étapes Z8X à X9Z est conservée, et la partie droite de l'algorithme de la figure 3 concernant les relations avec l'entité EY est remplacée par les étapes Y1 à Y9 à droite dans la figure 2, afin de comparer finalement la signature

SGXZ au résultat REXZ et la signature SGY au résultat REY à des étapes X9Z et Y9 avant de lire les données reçues DX et DY dans la carte CA à l'étape F9.

REVENDICATIONS

1 - Procédé pour sécuriser l'exécution d'une session avec un moyen de traitement de données (CA) sous la commande d'au moins deux entités électroniques (EX, EY), caractérisé en ce qu'il comprend les étapes suivantes de :

- transmettre (X2, Y2) des numéros de session (NSX, NSY) et des clés de session (KSX, KSY) depuis le moyen de traitement (CA) respectivement aux entités (EX, EY),

- appliquer (X6, X8 ; Y6, Y8) le numéro de session respectif (NSX, NSY) et la clé de session respective (KSX, KSY) à un algorithme de sécurisation respectif (ASX, ASY) dans le moyen de traitement (CA) et l'entité respective (EX, EY) pour produire un résultat respectif (REX, REY) et une signature respective (SGX, SGY),

- transmettre (X7, Y7) le numéro de session respectif (NSX, NSY) et la signature respective (SGX, SGY) depuis l'entité respective vers le moyen de traitement, et

- exécuter (F10) la session correspondant aux numéros de session retransmis (NSX, NSY) depuis le moyen de traitement (CA) lorsque les signatures sont respectivement identiques (X9, Y9) aux résultats.

2 - Procédé conforme à la revendication 1, selon lequel les résultats respectifs (REX, REY) sont écrits (X2, Y2) en mémoire dans le moyen de traitement (CA) respectivement en correspondance aux numéros de session respectifs (NSX, NSY) à transmettre aux entités (EX, EY), et sont lus (X9, Y9) en correspondance avec les numéros de session respectifs transmis par les entités vers le moyen de

traitement avant d'être comparés aux signatures respectives (SGX, SGY).

3 - Procédé conforme à la revendication 1 ou 2, selon lequel chacune des entités (EX, EY) transmet (X5, X7 ; Y5, Y7) vers le moyen de traitement (CA) des données respectives (DX, DY) avec le numéro de session respectif (NSX, NSY) et la signature respective (SGX, SGY), et la session est exécutée si, en outre, le moyen de traitement détecte dans chacune des données une acceptation de la session par l'entité respective.

4 - Procédé conforme à l'une quelconque des revendications 1 à 3, selon lequel, avant d'être transmis depuis le moyen de traitement (CA), le numéro de session respectif (NSX, NSY) et la clé de session respective (KSX, KSY) sont chiffrés (X3, Y3) par un algorithme de chiffrement respectif avec une clé publique respective (KPX, KPY) pour chacune des entités (EX, EY).

5 - Procédé conforme à l'une quelconque des revendications 1 à 4, selon lequel le moyen de traitement (CA) transmet (F9Y, F9Z) des accusés de réception respectif (ACKX, ACKY) aux entités respectives (EX, EY) au moins lorsque les signatures (SGX, SGY) sont respectivement identiques aux résultats (REX, REY).

6 - Procédé conforme à l'une quelconque des revendications 1 à 4, selon lequel le moyen de traitement (CA) produit (F11) un mot (ACK) représentatif de la session lorsque celle-ci doit être exécutée, des signatures de mot respectives

(SAX, SAY) résultant chacune de l'application dudit mot représentatif et de la clé de session respective (KSX, KSY) à l'algorithme de sécurisation respectif (ASX, ASY), pour transmettre (F12) le mot représentatif et les signatures de mot à l'une (EY) des entités afin qu'elle vérifie (F13) la correspondance entre le mot représentatif (ACK) et la signature de mot respective (SAY) en fonction de la clé de session respective (KSY) et, lorsqu'il y a correspondance, transmette (F14) ledit mot représentatif (ACK) et les autres signatures de mot respectives (SAX) à une autre entité (EX), laquelle vérifie (F15) la correspondance entre le mot représentatif (ACK) et la signature de mot respective (SAX) en fonction de la clé de session respective (KSX), et ainsi de suite jusqu'à la dernière entité.

7 - Procédé conforme à l'une quelconque des revendications 1 à 6, comprenant préalablement une authentification (X1, Y1) du moyen de traitement (CA) par les entités (EX, EY) et/ou inversement.

8 - Procédé conforme à l'une quelconque des revendications 1 à 7, comprenant les étapes suivantes de :

- transmettre (Z2) des informations de délégation respectives (IDX, IDY) en faveur de l'une desdites au moins deux entités (EX, EY) depuis une troisième entité électronique (EZ) au moyen de traitement (CA),

- transmettre (Z4, Z5) un numéro de session (NS), lequel est identique aux numéros de session respectifs (NSX, NSY), et une troisième clé de session (KSZ) depuis le moyen de traitement (CA) à la troisième entité prédéterminées (EZ),

- retransmettre (Z7) le numéro de session (NS) et la troisième clé de session (KSZ) par la troisième entité (EZ) vers ladite une entité (EX), et

- appliquer (X6Z) non seulement le numéro de session (NS) et la clé de session respective (KSX) pour ladite une entité (EX) mais également la troisième clé de session (KSZ) à l'algorithme de sécurisation respectif (ASX) dans ladite une entité (EX) et le moyen de traitement (CA) pour produire la signature respective (SGX) et le résultat respectif (REX).

9 - Procédé conforme à la revendication 8, selon lequel les informations de délégation (IDX, IDY) sont signées avec une clé privée de la troisième entité (EZ), puis chiffrées avec une clé publique (KPCA) du moyen de traitement (CA).

10 - Procédé conforme à la revendication 8 ou 9, selon lequel le numéro de session (NS) retransmis (Z7) par la troisième entité (EZ) et le numéro de session transmis (X2) directement par le moyen de traitement (CA) à ladite une entité (EX) sont comparés (Z9X) dans ladite une entité (EX), et au moins l'étape d'appliquer (X6Z) dans ladite une entité n'est exécutée que lorsque les numéros de session comparés sont identiques.

11 - Procédé conforme à l'une quelconque des revendications 8 à 10, selon lequel avant d'être transmis et retransmis (Z5, Z7), le numéro de session (NS) et la troisième clé de session (KSZ) sont chiffrés avec une troisième clé publique (KPZ) de la troisième entité (EZ), puis avec une clé publique (KPX) de ladite une entité (EX).

12 - Procédé conforme à l'une quelconque des revendications 8 à 11, selon lequel au moins une autre entité (EY) desdites au moins deux entités est déléguée de la troisième entité (EX) afin que la session ne soit exécutée que lorsque les signatures (SGXZ, SGYZ) et les résultats (REXZ, REYZ) produits en fonction du numéro de session (NS), des clés de session respectives (KSX, KSY) et de la troisième clé de session (KSZ) sont respectivement identiques.

13 - Procédé conforme à l'une quelconque des revendications 1 à 12, selon lequel le moyen de traitement (CA) et/ou au moins l'une des entités (EX, EY, EZ) est une carte à puce.

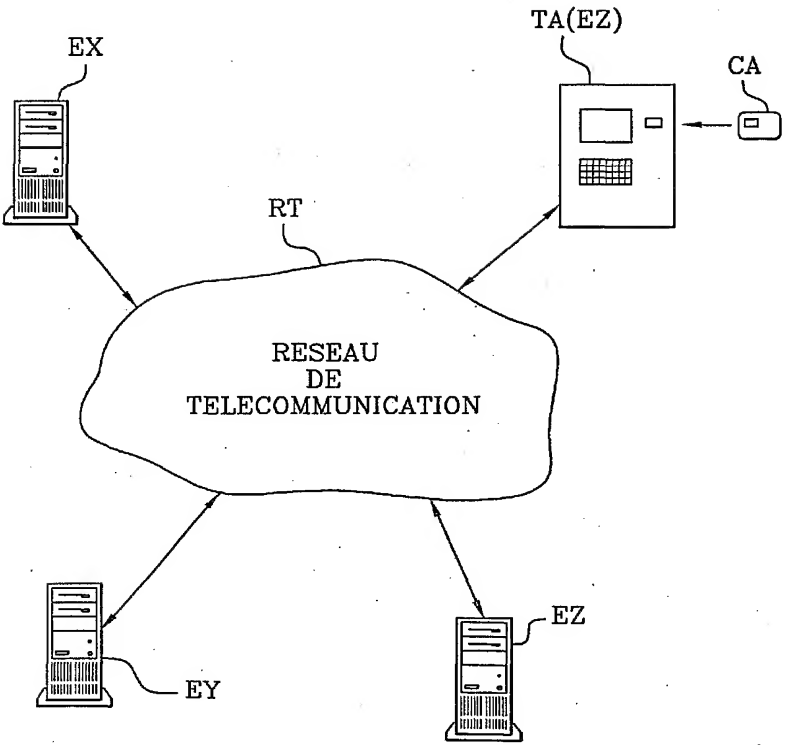


Fig. 1

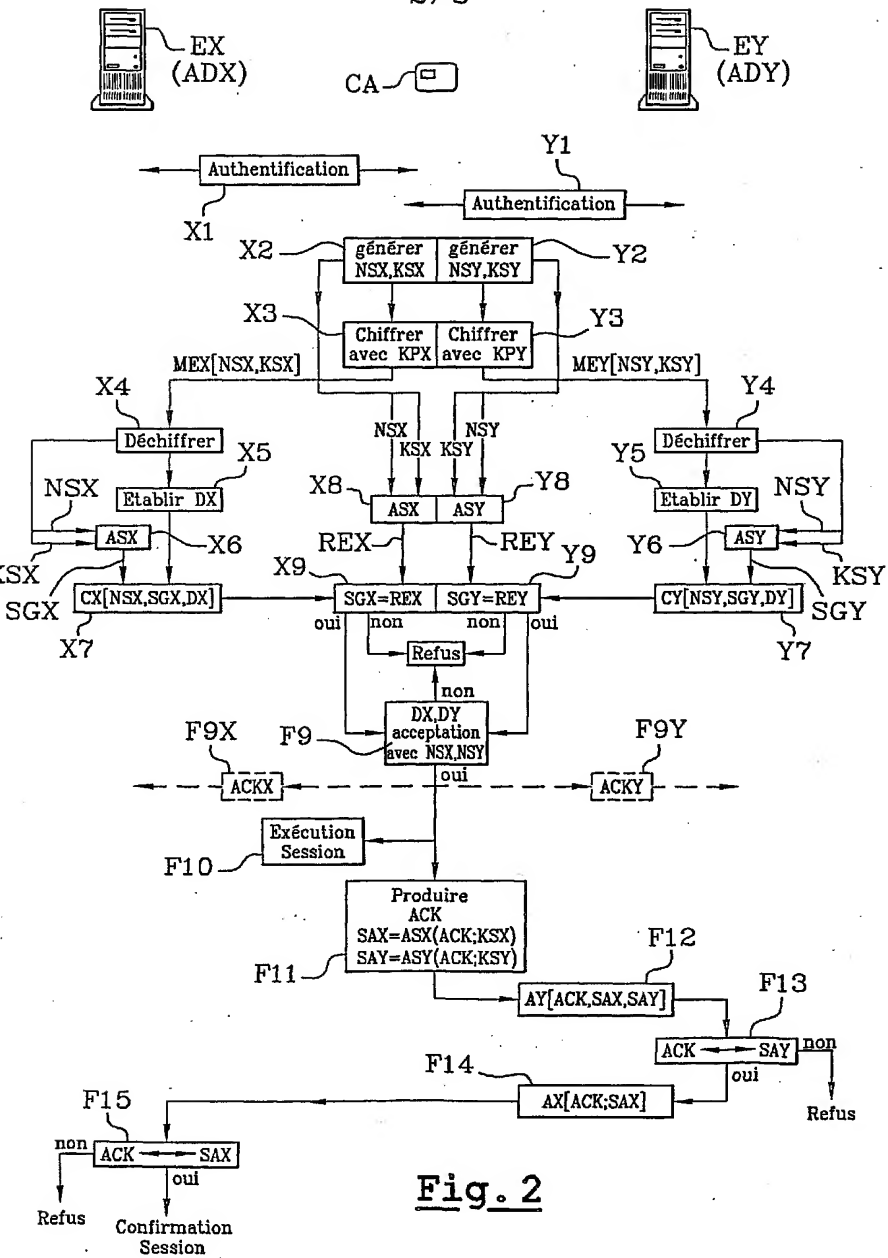

EX
(ADX)
CA
EY
(ADY)
Authentification
Authentification
Y1
X1
X2
générer NSX,KSX
générer NSY,KSY
Y2
X3
Chiffrer avec KPX
Chiffrer avec KPY
Y3
MEX[NSX,KSX]
MEY[NSY,KSY]
X4
Y4
Déchiffrer
Déchiffrer
NSX
KSX
NSY
KSY
X5
Y5
Etablir DX
Etablir DY
X8
Y8
ASX
ASY
REX
REY
X9
Y9
Y6
KSX
KSY
SGX
SGY
CX[NSX,SGX,DX]
SGX=REX
SGY=REY
CY[NSY,SGY,DY]
X7
Y7
oui
non
non
oui
Refus
non
DX,DY acceptation avec NSX,NSY
F9X
F9
F9Y
ACKX
ACKY
oui
Exécution Session
F10
Produire ACK
SAX=ASX(ACK;KSX)
SAY=ASY(ACK;KSY)
F11
F12
AY[ACK,SAX,SAY]
F13
ACK SAY
non
oui
Refus
F14
AX[ACK;SAX]
F15
non
ACK SAX
oui
Refus
Confirmation Session

Fig. 2

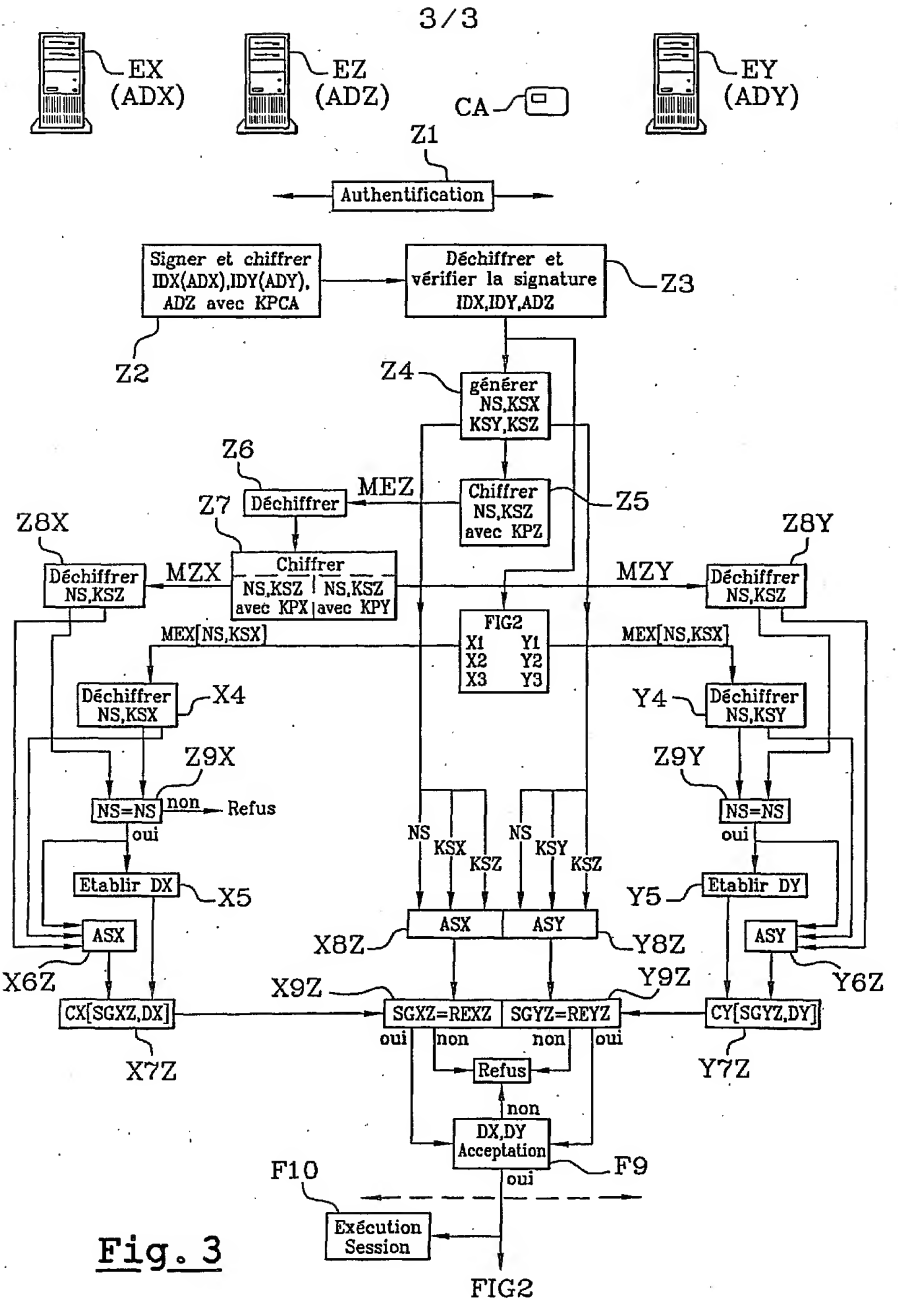

EX
(ADX)
EZ
(ADZ)
CA
EY
(ADY)
Z1
Authentification
Signer et chiffrer IDX(ADX),IDY(ADY), ADZ avec KPCA
Z2
Déchiffrer et vérifier la signature IDX,IDY,ADZ
Z3
Z4
générer NS,KSX KSY,KSZ
Z6
Déchiffrer
MEZ
Chiffrer NS,KSZ avec KPZ
Z5
Z7
Z8X
Z8Y
Déchiffrer NS,KSZ
MZX
Chiffrer
NS,KSZ avec KPX
NS,KSZ avec KPY
MZY
Déchiffrer NS,KSZ
FIG2
X1 Y1
X2 Y2
X3 Y3
MEX[NS,KSX]
MEX[NS,KSX]
Déchiffrer NS,KSX
X4
Y4
Déchiffrer NS,KSY
Z9X
Z9Y
NS=NS
non
Refus
oui
NS=NS
oui
NS KSX KSZ
NS KSY KSZ
Etablir DX
X5
Y5
Etablir DY
ASX
ASX
ASY
ASY
X8Z
Y8Z
X6Z
X9Z
Y9Z
Y6Z
CX[SGXZ,DX]
SGXZ=REXZ
SGYZ=REYZ
CY[SGYZ,DY]
oui
non
non
oui
Refus
non
DX,DY Acceptation
F9
F10
oui
Exécution Session
X7Z
Y7Z
FIG2

Fig. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/02454

A. CLASSIFICATION OF SUBJECT MATTER
IPC- 7 H04L9/32 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	ME L ET AL: "LE COMMERCE ELECTRONIQUE: UN ETAT DE L'ART" ANNALES DES TELECOMMUNICATIONS - ANNALS OF TELECOMMUNICATIONS,CH,PRE SSES POLYTECHNIQUES ET UNIVERSITAIRES ROMANDES, LAUSANNE, vol. 53, no. 9/10, 1 September 1998 (1998-09-01), pages 361-376, XP000791619 ISSN: 0003-4347 page 371 -page 372	1-5,7,13
A	--- -/--	6,8

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
8 October 2001	12/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/02454

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	MENEZES , OORSCHOT, VANSTONE: "Handbook of Applied Cryptography" CRC PRESS,US, 1997, XP002173212 BOCA RATON, FL, US ISBN: 0-8493-8523-7 page 403 -page 405 page 506 -page 509	1-5,7,13

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 01/02454

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G07F G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, INSPEC, PAJ, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	ME L ET AL: "LE COMMERCE ELECTRONIQUE: UN ETAT DE L'ART" ANNALES DES TELECOMMUNICATIONS - ANNALS OF TELECOMMUNICATIONS,CH,PRE SSES POLYTECHNIQUES ET UNIVERSITAIRES ROMANDES, LAUSANNE, vol. 53, no. 9/10, 1 septembre 1998 (1998-09-01), pages 361-376, XP000791619 ISSN: 0003-4347 page 371 -page 372	1-5,7,13
A	--- -/--	6,8

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
8 octobre 2001	12/10/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Carnerero Álvaro, F

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

De[illegible]de internationale No
PCT/FR 01/02454

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
Y	MENEZES , OORSCHOT, VANSTONE: "Handbook of Applied Cryptography" CRC PRESS,US, 1997, XP002173212 BOCA RATON, FL, US ISBN: 0-8493-8523-7 page 403 -page 405 page 506 -page 509	1-5,7,13

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (juillet 1992)